Rx: Health Care FYI #28

Subject: *Protecting Patient Privacy for the 21st Century*

From: *Rep. Tim Murphy (PA-18)*

The problem: Your medical records are more vulnerable than you think. The current privacy law, enacted in 1996, may fall short of meeting the needs for health information technology, which stores medical records on computer files.

- More than *one in four* health insurance plans (payers) and almost *one in three* providers (doctors and hospitals) have indicated that their organizations experienced data security breaches by computer hackers from January-June 2005.
- Only 43% of health care providers have achieved compliance with federal laws that protect the unauthorized disclosure of personal health information. [1]
- As an example of a health data security breach, a temporary employee of a cancer center stole patients' personal information. The employee allegedly used one patient's name and data to obtain $2,500 in long distance and other phone service.[2]
- As another example of data security failure, about 400 pages of detailed psychological records concerning visits and diagnoses of at least 62 children and teenagers were accidentally posted on a website for eight days. The information included names, dates of birth and, in come cases, home addresses and schools attended, along with psychological test results.[3]

The current Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996. Your personal health care information <u>can be</u> legitimately used by:

- Doctors and hospitals for treatment and coordination of care with patient consent.
- Individuals whom the patient grants legal consent to pay your health care bills.
- Federal, state and local authorities can use general health information to protect the public health, such as by reporting when the flu is in your area.
- Law enforcement in order to make required reports to the police, such as reporting gunshot wounds, and child abuse cases.[4]

Your health information <u>cannot be</u> used or shared without your written permission, unless HIPAA allows it. For example, without your authorization, your health care provider generally cannot:

- Give your information to your employer.
- Use or share your information for marketing or advertising purposes.

---

[1] HIMSS/Phoenix Health Systems: U.S. Healthcare Industry HIPAA Survey Results: Summer 2005

[2] J. Ellement, "Dana-Farber Says Patient Data Stolen," *The Boston Globe*, August 8, 2000, p. A1.

[3] C. Piller, "Web Mishap: Kids' Psychological Files Posted," *Los Angeles Times*, November 7, 2001, p. A1.

[4] U.S. Department of Health and Human Services. Privacy and Your Health Information. Fact Sheet. July 2005.

- Share private notes about your mental health counseling session.4

The Federal Government's Role:

- In 1996, Congress passed HIPAA, which establishes privacy protections for patients by limiting the ways that health care providers can use patients' personal medical information.
- HHS has issued electronic format and data standards for payments between plans and providers and security standards to safeguard electronic patient information against unauthorized access, use, and disclosure. Health plans had until April 21, 2005, to comply.

What can a person do if their data is misused?

- **Penalties:** ***Enforcement of HIPAA is currently reactive and complaint-driven.*** The civil fines are $100 per incident, capped at $25,000 per year for each provision that is violated. The criminal penalties include fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer or use it for commercial advantage, personal gain, or malicious harm.
- **Complaints:** Consumers may file a formal complaint regarding the privacy practices of a covered health plan or provider to HHS' Office for Civil Rights (OCR). Consumers can find out more information about filing a complaint at http://www.hhs.gov/ocr/hipaa or by calling (866) 627-7748.

Recommendations for Congress:

- Provide the resources necessary for HHS to shift from the current complaint-driven, reactive enforcement of privacy standards to a proactive enforcement to protect patient privacy and confidentiality for adequate oversight as we move towards electronic medical records.
- Congress needs to update current laws to meet the needs of electronic medical records. H.R. 2234, the 21st Century Health Information Act establishes privacy provisions to keep electronic medical records secure. Patients must have access to their own records, be allowed to opt out of pilot programs for a national health information network, technology should only allow general patient information and Congress should require notification of the unauthorized access or disclosure of individually identifiable patient health information to affected or possibly affected patients as well as the Secretary of HHS.
- Ensure a seamless transition of general public health information to a patient safety organization (PSO) under the Patient Safety and Quality Improvement Act of 2005 (Public Law: 109-41).
- Implement the universal privacy study in H.R. 4157, the Health Information Technology Promotion Act. This would require HHS to decide if uniform privacy standards were needed.
- Provide assistance to small physician practices and home health care providers to meet federal privacy standards for health information technology.